Annual 47 CFR § 64.2009(e) CPNI Certification

EB Docket
06-36

Annual 64.2009(e) CPNI Certification for 2019 covering the prior calendar year 2018

1. Date filed: Feb. 20, 2019
2. Name of company(s) covered by this certification: Five9, Inc.
3. Form 499 Filer ID: 829544
4. Name of signatory: Scott Welch
5. Title of signatory: Executive Vice President, Cloud Operations and Platform Engineering
6. Certification:

I, Scott Welch, certify that I am an officer of the company named above, and acting as an agent of the company, that I have personal knowledge that the company has established operating procedures that are adequate to ensure compliance with the Commission's CPNI rules. *See* 47 CFR § 64.2001 *et seq*.

Attached to this certification is an accompanying statement explaining how the company's procedures ensure that the company is in compliance with the requirements (including those mandating the adoption of CPNI procedures, training, safeguards, recordkeeping, and supervisory review) set forth in section 64.2001 *et seq.* of the Commission's rules.

The company has not taken actions (i.e., proceedings instituted or petitions filed by a company at either state commissions, the court system, or at the Commission against data brokers) against data brokers in the past year.

The company has not received customer complaints in the past year concerning the unauthorized release of CPNI.

The company had one incident on July 26, 2018 resulting in the inadvertent delivery of CPNI information to the wrong customer. The customer who received the information in error, promptly deleted the data and provided a signed statement of destruction.

The company represents and warrants that the above certification is consistent with 47 CFR § 1.17, which requires truthful and accurate statements to the Commission. The company also acknowledges that false statements and misrepresentations to the Commission are punishable under Title 18 of the U.S. Code and may subject it to enforcement action.

Signed: 

Date 2/20/19

Attachments: Accompanying Statement explaining CPNI procedures
Summary of CPNI Incident

STATEMENT REGARDING CUSTOMER PROPRIETARY INFORMATION OPERATING PROCEDURES

Five9, Inc.

Five9, Inc. ("Five9") in accordance with Section 64.2009(e) submits this statement summarizing how its operating procedures are designed to ensure compliance with the Commission's CPNI rules.

Use of CPNI by Five9

Five9 values its customers' privacy and takes measures to protect CPNI. It is Five9's policy to protect the confidentiality of its customers' information. Five9 does not use, disclose or permit access to its customers' CPNI except as such use, disclosure or access is permitted under Section 222 of the Communications Act of 1934, as amended, and the Commissions implementing rules. As necessary, Five9 may use CPNI for the permissible purposes enumerated in the Act and the Commission's rules, including, but not limited to, initiating, rendering, billing and collecting for its services. Five9 may also use CPNI to protect its rights or property. Five9 does not utilize CPNI to market its services.

Five9 employees will disclose personal data to third parties only for valid business reasons. The customer's implicit or explicit consent will be obtained when required. In addition to the execution of a nondisclosure agreement for the protection of confidential information, Five9 will require a commitment by third parties receiving CPNI to adhere to the Five9 Privacy and Data Protection policies and all related procedures to protect CPNI.

Data Protection

Five9 has written policies to protect its customer data integrity, availability and confidentiality. All Employees are instructed on the proper use and protection of customer data. Further, employees are aware of express disciplinary consequences for failing to protect customer data, and are responsible for notifying their managers, who, in turn, are required to notify the Information Security Group of any potential breach. Five9's Information Security Group maintains a policy of conducting security audits to ensure that data is protected.

Data Breaches

In the event that Five9 experiences a data breach, Five9 has appointed a management representative to serve as liaison with law enforcement, as required, and to coordinate these efforts with the Information Security Group. Further, Five9 has written procedures in place to respond if a data breach takes place. Employees are instructed not to discuss a possible breach with any party outside of Five9's Information Security Group.

Five9 will maintain record of any data breach for a minimum of three years.

Password Protection

Customer contracts provide for security of confidential information, including the establishment of a password to authenticate the customer's identity prior to access to CPNI. In the alternative, the customer may establish security questions upon account set-up. Further, the customer agreements require a customer to designate up to three specific customer contacts with whom Five9 may discuss issues with the customer's account. Any account inquiries from non-qualified customer contacts will be denied. All customer agreements contain strict confidentiality provisions.

Summary of CPNI Incident July 26, 2018

Five9, Inc. ("Five9") reported a CPNI incident via the Data Breach Reporting Portal in July 2018.

Summary of Incident

On July, 26, 2018 a Five9 service agent, who was working on multiple customer requests, inadvertently sent the wrong customer a call log report. The information sent include call log details for calls between Nov. 2017 and May 2018 for one customer. The CPNI data elements in the report included: call date, call time, DNIS, ANI and call duration. The file name identified the customer name. The file detail did not include agent or customer names.

The customer, who received the call log report in error, promptly deleted the information from their systems and provided Five9 with a signed statement of destruction.